Wed, 17 Nov 16h00 – 17h50	**Workshop 8 – Cybercrime, e-evidence and artificial intelligence** Languages: EN/FR/SP Purpose: Rapid progress in AI raises: ▪ additional risks of cybercrime (offenders weaponizing AI, AI detecting vulnerabilities to commit cybercrime or automate attacks. AI as target manipulated by offenders) ▪ questions of criminal liability (who is liable for decisions made and crime committed through AI technology?) ▪ complex challenges related to electronic evidence (how can e-evidence related to crime involving AI be secured and used in criminal proceedings?) On the other hand, AI may bring benefits to the criminal justice response to cybercrime (improving cybersecurity; detecting attacks; helping identify, investigate and prosecute offenders; or automating domestic and international cooperation). However, this in turn raises additional questions (how can rule of law and due process safeguards be ensured; what implications on territoriality and jurisdiction when AI-led investigations cross borders?). Organisations worldwide are currently working on questions related to artificial intelligence, including the Council of Europe. Within this context, the aim of the workshop is to identify key issues that should be taken into account when designing the future criminal justice response to cybercrime and e-evidence in relation to AI. Moderator/s: Jan Kleijssen (Director of Information Society and Action against Crime, Council of Europe) Rapporteur: Tania Schröter (Deputy Head of Unit, Procedural Criminal Law, Directorate-General for Justice and Consumers, European Union Commission) Secretariat: Martha Stickings / Gratiela Dumitrescu (GLACY+, C-PROC, Council of Europe) ► **Introduction and objective of the workshop** – Jan Kleijssen (Council of Europe) ► **Cybercrime and artificial intelligence: what are the threats and challenges, what are the opportunities?** – Malicious uses and abuses of artificial intelligence (Aglika Klayn, Cybercrime Specialist/J-CAT Coordinator, EC3, EUROPOL / Maria Eira, UNICRI Centre for AI and Robotics / David Sancho, TrendMicro) – Provenance tech (Origin and C2PA) techniques and lessons learned from disinformation countermeasures (Ashish Jaiman, Director of Product Management, Microsoft) – Discussion ► **AI, cybercrime and the law: fundamentals**

	– AI, cybercrime and criminal law: what is new and what is not new? (Dennis Baker, Professor, De Montfort University Law School, Leicester, UK) – AI, e-evidence and criminal liability (Sabine Gless, CDPC rapporteur on AI and Criminal Law, Professor of criminal law and criminal procedure law, University of Basel, Switzerland) – Discussion ► **Conclusions**